MATHS 255 Class Notes
Natural numbers, integers, divisibility
(7.1, 7.2)

Division Algorithm (7.2.1)
For all $m \in \mathbf{Z}$, $n \in \mathbf{N}$, there exists unique $q \in \mathbf{Z}$, $r \in \{0, \cdots, n-1\}$ such that $p \in \mathbf{Z}$ $m = nq + r$.

[q = quotient, r = remainder]

Divisibility
For all $m, n \in \mathbf{Z}$, we say "m divides n" (written $m \mid n$) if for some $r \in \mathbf{Z}$, $mr = n$.

Basic properties:
$\forall a, b, c \in \mathbf{Z}$

1. $a \mid a$
2. $\pm 1 \mid a$
3. $a \mid 0$
4. If $a \mid b$ then $a \mid -b$
5. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.
6. If $a \mid b$ and $b \mid a$ then $a = \pm b$.
7. If $a \mid b$ and $b \mid c$ then $a \mid c$.

"Divides" is a partial ordering on the set of natural numbers (but not on the set of integers).

Primes
$p \in \mathbf{Z}$ is *prime* if $p > 1$ and its only positive divisors are $1, p$.

The prime numbers are the minimal elements in $\mathbf{N} \setminus \{1\}$ under the relation of "divides".

Theorem. The number of primes is infinite.
(Indirect proof)